

APPENDIX A

AMENDED CLAIMS – S/N 09/584,162

1. (Twice Amended) A pointing device comprising:

- an interface for operably communicating with an electronic system;
- a position sensor, responsive to user movement thereof, for conveying positional information by way of said interface to the electronic system;
- a user-depressable button for conveying selection information by way of said interface to the electronic system;
- a biometric sensor disposed at a location such that when operating said pointing device in a normal manner a user's hand rests naturally in a position to place a finger of the user's hand in proximity to and readable by said biometric sensor; and
- a verification system for operably communicating with the electronic system, the verification system comprising a user storage, an authorization profile storage, and an audit log storage, the audit log storage being configured to store:
 - (a) user identification information from said biometric sensor in response to [an unsuccessful transaction attempt and] a denial of access [with] to said electronic system; and
 - (b) user identification information from said biometric sensor and attempted transaction information in response to a denial of access to perform a specific transaction within said electronic system.

61. (Amended) A pointing device comprising:

- an interface for operably communicating with an electronic system;
- a position sensor, responsive to user movement thereof, for conveying positional information by way of said interface to the electronic system;
- a user-depressable button for conveying selection information by way of said interface to the electronic system; and
- a biometric sensor disposed at a location such that when operating said pointing device in a normal manner a user's foot rests naturally in a position to place a toe of the user's foot in proximity to and readable by said biometric sensor; and

a verification system for operably communicating with the electronic system, the verification system comprising a user storage, an authorization profile storage, and an audit log storage, the audit log storage being configured to store:

- (a) user identification information from said biometric sensor in response to [an unsuccessful transaction attempt and] a denial of access [with] to said electronic system; and
- (b) user identification information from said biometric sensor and attempted transaction information in response to a denial of access to perform a specific transaction within said electronic system.

67. (Amended) A computer verification system for use with a biometric sensor, said verification system comprising:

a processor coupled to the biometric sensor; and

a memory coupled to the processor, the memory comprising:

a user storage and an authorization profile being configured to verify an identification of a user each time the user inputs a request to an electronic system; and

an audit log storage being configured to store:

- (a) user identification information from the biometric sensor in response to [an unsuccessful transaction attempt and] a denial of access [with] to the electronic system; and
- (b) user identification information from said biometric sensor and attempted transaction information in response to a denial of access to perform a specific transaction within said electronic system.

71. (Amended) A method for verifying a user of an electronic system coupled to a biometric sensor, the method comprising:

obtaining user identification information of the user with the biometric sensor;

obtaining a selection of the user for the electronic system;

comparing the user identification information with information stored in a user storage;

comparing the selection with authorization information stored in an authorization profile;

determining if the user is authorized to perform the selection; and
storing identification information and attempted transaction information of the user in the
audit log storage if the user is [not authorized] denied access to perform the
[selection and is denied access to] selection within the electronic system.

79. (Amended) A verification system for operably communicating with an electronic system,
the verification system comprising a user storage, an authorization profile storage, and an audit
log storage, the audit log storage being configured to store information in response to a
successful transaction attempt and grant of access with said electronic system and to [an
unsuccessful transaction attempt and] a denial of access [with] to said electronic system and
denials of access to perform specific actions within said electronic system.

APPENDIX B

PENDING CLAIMS – S/N 09/584,162

1. A pointing device comprising:
 - an interface for operably communicating with an electronic system;
 - a position sensor, responsive to user movement thereof, for conveying positional information by way of said interface to the electronic system;
 - a user-depressable button for conveying selection information by way of said interface to the electronic system;
 - a biometric sensor disposed at a location such that when operating said pointing device in a normal manner a user's hand rests naturally in a position to place a finger of the user's hand in proximity to and readable by said biometric sensor; and
 - a verification system for operably communicating with the electronic system, the verification system comprising a user storage, an authorization profile storage, and an audit log storage, the audit log storage being configured to store:
 - (a) user identification information from said biometric sensor in response to a denial of access to said electronic system; and
 - (b) user identification information from said biometric sensor and attempted transaction information in response to a denial of access to perform a specific transaction within said electronic system.
2. A pointing device as recited in claim 1, wherein the biometric sensor comprises a fingerprint sensor.
7. A pointing device as recited in claim 1, wherein said biometric sensor is configured to convey a digitized scanned image of the user's fingerprint to said electronic system.
8. A pointing device as recited in claim 1, wherein said biometric sensor is configured to convey a compressed digital representation of the user's fingerprint to said electronic system.

9. A pointing device as recited in claim 1, wherein said biometric sensor is configured to convey a digital representation of a minutia of the user's fingerprint to said electronic system.
10. A pointing device as recited in claim 1 wherein the position sensor comprises a mouse.
11. A pointing device as recited in claim 2:
further comprising at least one button position; and
wherein the fingerprint sensor is disposed below a particular one of the at least one button positions.
12. A pointing device as recited in claim 11 wherein an operable button is located at the particular button position.
13. A pointing device as recited in claim 11 wherein an inoperable button is located at the particular button position.
14. A pointing device as recited in claim 11 wherein no button is located at the particular button position.
15. A pointing device as recited in claim 11 wherein:
the at least one button positions numbers three; and
the fingerprint sensor is disposed below a centermost button position of the three button positions.
16. A pointing device as recited in claim 1 wherein the position sensor comprises a trackball.
17. A pointing device as recited in claim 16 wherein the position sensor further includes a second trackball.
18. A pointing device as recited in claim 1, wherein the position sensor comprises a trackball that is movably-connected to the pointing device so that the trackball is positionable to either

side of the biometric sensor so that the pointing device is equally well suitable for use by either a right-handed or a left-handed user.

19. A pointing device as recited in claim 18 wherein the trackball is rotatably-connected to the pointing device.

20. A pointing device as recited in claim 1 wherein the interface comprises a cabled interface.

21. A pointing device as recited in claim 1 wherein the interface comprises a wireless interface.

22. A pointing device as recited in claim 11 wherein:

the fingerprint sensor includes an optical imaging array; and

the particular button position includes a transparent material through which the user's fingerprint may be imaged by the imaging array.

23. A pointing device as recited in claim 11 wherein:

the fingerprint includes a capacitive imaging array located at the particular button position contactable by the user's finger so that the user's fingerprint may be imaged by the capacitive imaging array.

24. A pointing device as recited in claim 23 wherein:

the fingerprint sensor is incorporated into an operable button located at the particular button position.

49. A pointing device as recited in claim 1, wherein the user storage, the authorization profile storage, and the audit log storage comprise one or more memory devices.

50. The pointing device of claim 49, wherein the one or more memory devices comprise a CD-ROM, a magnetic disk, an optical disk, or a flash memory.

51. The pointing device of claim 1, wherein the user storage, the authorization profile storage, or the audit log storage comprise a removable memory device.

52. The pointing device of claim 1, wherein the user storage, the authorization profile storage, or the audit log storage store encoded information.

53. The pointing device of claim 1, wherein the authorization profile storage stores permissible dates, times, functions, transactions, or any combination thereof associated with a user of said electronic system.

54. The pointing device of claim 1, wherein the audit log storage stores transaction information for a user who successfully accessed said electronic system.

55. The pointing device of claim 1, wherein the audit log storage stores a record of successful and unsuccessful system accesses to said electronic system.

56. The pointing device of claim 1, further comprising a substance detection sensor in operative relation with the biometric sensor.

57. The pointing device of claim 56, wherein the substance detection sensor detects narcotics, blood alcohol content, or any combination thereof of the user.

58. The pointing device of claim 57, wherein the verification system is configured to authorize or prevent access to the electronic system according to the user's blood alcohol content.

59. The pointing device of claim 56, wherein at least a portion of the substance detection sensor overlaps the biometric sensor.

60. The pointing device of claim 1, further comprising one or more additional biometric sensors in operative relation with the user and coupled to said interface.

61. A pointing device comprising:

- an interface for operably communicating with an electronic system;
- a position sensor, responsive to user movement thereof, for conveying positional information by way of said interface to the electronic system;
- a user-depressable button for conveying selection information by way of said interface to the electronic system; and
- a biometric sensor disposed at a location such that when operating said pointing device in a normal manner a user's foot rests naturally in a position to place a toe of the user's foot in proximity to and readable by said biometric sensor; and
- a verification system for operably communicating with the electronic system, the verification system comprising a user storage, an authorization profile storage, and an audit log storage, the audit log storage being configured to store:
 - (a) user identification information from said biometric sensor in response to a denial of access to said electronic system; and
 - (b) user identification information from said biometric sensor and attempted transaction information in response to a denial of access to perform a specific transaction within said electronic system.

67. A computer verification system for use with a biometric sensor, said verification system comprising:

- a processor coupled to the biometric sensor; and
- a memory coupled to the processor, the memory comprising:
 - a user storage and an authorization profile being configured to verify an identification of a user each time the user inputs a request to an electronic system; and
 - an audit log storage being configured to store:
 - (a) user identification information from the biometric sensor in response to a denial of access to the electronic system; and
 - (b) user identification information from said biometric sensor and attempted transaction information in response to a denial of access to perform a specific transaction within said electronic system.

68. The verification system of claim 67, wherein the memory comprises a CD-ROM, a magnetic disk, an optical disk, or a flash memory.

69. The verification system of claim 67, wherein the memory comprises a removable memory device.

70. The verification system of claim 67, wherein the memory stores encoded information.

71. A method for verifying a user of an electronic system coupled to a biometric sensor, the method comprising:

- obtaining user identification information of the user with the biometric sensor;
- obtaining a selection of the user for the electronic system;
- comparing the user identification information with information stored in a user storage;
- comparing the selection with authorization information stored in an authorization profile;
- determining if the user is authorized to perform the selection; and
- storing identification information and attempted transaction information of the user in the audit log storage if the user is denied access to perform the selection within the electronic system.

72. The method of claim 71, wherein the authorization information comprises permissible dates, times, functions, transactions, or any combination thereof associated with the user.

73. The method of claim 71, wherein storing identification information or storing transaction information comprises storing encoded information.

74. The method of claim 71, wherein the authorization information stored in the authorization profile is stored by one or more persons other than the user.

75. The method of claim 71, further comprising detecting a substance of the user with a substance detection sensor to determine if the user is authorized to access the electronic system.

76. The method of claim 75, wherein the substance comprises a narcotic or alcohol.

77. The method of claim 71, further comprising detecting a substance of the user with a substance detection sensor to determine if the user is authorized to perform the selection.

78. The method of claim 77, wherein the substance comprises a narcotic or alcohol. --

79. A verification system for operably communicating with an electronic system, the verification system comprising a user storage, an authorization profile storage, and an audit log storage, the audit log storage being configured to store information in response to a successful transaction attempt and grant of access with said electronic system and to a denial of access to said electronic system and denials of access to perform specific actions within said electronic system.

80. The verification system of claim 79, wherein the information comprises digital information.

81. The verification system of claim 79, wherein the information comprises encoded information.